디지털산업정보학회 논문지 제19권 제2호-2023년 6월
http://dx.doi.org/10.17662/ksdim.2023.19.2.089

산업별 정보보안의 투자 수준과 관리 역량에 관한 연구*

정 병 호** · 주 형 근***

A Study on the Investment Level and Administrative Competence of Information Security by Industry

Jung Byoungho · Joo Hyungkun

〈Abstract〉

The purpose of this study is to examine what are the important variables for information security compliance and whether the information security investment by the industry is different. To comply with the information security policies, the organization must establish measures to prevent or resolve information security incidents. This research process consists of four stages, and the analysis method was conducted with the categorical regression analysis and the correspondence analysis. The first analysis analyzed the independent variables that affect security regulations compliance. The rest of the analysis was conducted by industry in the order of security compliance regulations, manpower investment, and budget investment. As a result of the first analysis, this had positive effects on an organization and personal information protection awareness, joint operation organization of information protection, manpower and budget investment, corporate size, and industry. The correspondence analysis was conducted from the second analysis to the fourth analysis and it analyzed the differences in information security investment by industry. The second analysis showed that the construction industry, science and technology industry, and finance industry have higher compliance with security regulations than other industries. The third analysis showed that the financial industry and the science and technology industry were higher than other industries. The last analysis showed that the financial industry was higher than other industries. The theoretical contribution of this study provided the basis for updating the information security theory. The practical contribution of this study requires government support to reduce information security deviations by industry.

Key Words : Information Security, Confidential Information, Information Security Investment, Administrative Security, Information Security Competence

* 본 연구는 한성대학교 교내학술연구비 지원과제임
** 상지대학교 빅데이터사이언스학과 외래교수 (제1저자)
*** 한성대학교 지식서비스&컨설팅대학원 교수 (교신저자)

Ⅰ. 서론

빅데이터 분석과 인공지능 활용이 보편화되면서 사회·경제적 관점에서 데이터와 정보의 관리가 매우 중요해지고 있다. 첨단기술과 기밀정보는 기업의 경쟁력에도 중요한 자산이지만 국가 경제에도 상당한 영향을 제공한다. 그래서 해킹과 내부 조직 구성원들을 통한 기밀정보 유출은 매년 발생하고 있다. 최근 2023년 5월 17일 언론보도에 따르면 삼성전자에서 반도체 핵심 자료 유출이 발생하는 사고가 있었으며[1], 테슬라 역시 10만 명 이상의 개인정보보호 유출이 발생하는 사고가 나타났다[2]. 또한 애플과 삼성의 경우 내부정보 유출을 우려하여 ChatGPT 사용을 금지하고 있다[3]. 이처럼 핵심 기밀정보는 기업의 지속가능 경영과 장기적 경영전략에 매우 중요한 자산으로 자리매김하고 있다.

한편, 정보기술이 고도화되면서 해킹의 기술도 함께 수준이 높아지고 있으며 내부 직원들의 비윤리적 행동으로 인하여 기밀정보가 유출되는 경우도 비일비재하게 발생하고 있다[4]. 기밀정보는 기업 경쟁력을 강화하는 데 매우 중요한 자산으로 인식되고 있어서 기업들의 정보보안 인식도 높아지고 있는 추세이다. 특히 기업 기밀정보 유출에 따른 정보사고 연구에서도 관리적 보안이 중요하다고 강조하고 있다[5]. 관리적 보안은 정보보안 교육, 정보보안 정책, 절차, 규정 등의 내용이 포함되며 기업의 필수적인 관리 역량이라고 할 수 있겠다[6]. 기업은 정보보안 관리 역량 강화와 정보사고를 미리 방지하고자 정보보안 교육도 정기적으로 수행하고 있다[7].

하지만 정보보안의 중요성을 강조하고 있는 상황에서도 기업의 기밀정보 유출은 지속해서 발생하고 상황이다. 이에 따라 정보보안 준수에 필요한 중요 변수가 무엇인지 살펴보고, 산업별로 정보보안 투자에서도 차이가 있는지를 살펴보고자 한다.

Ⅱ. 이론적 배경

2.1 기밀정보 유출

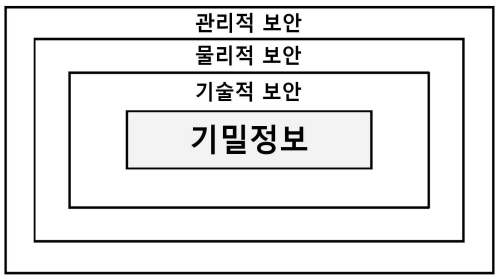
기업의 기밀정보란 정보의 열람에 접근권한이 부여된 정보를 말하며, 허가된 인적자원만 정보를 열람할 수 있고, 비인가 된 인적자원에 대하여는 정보의 접근을 차단하는 것을 말한다[8]. 기밀정보는 기업의 경영활동에 상당한 영향력을 가진 정보로서 외부에 유출되면 해당 기업은 재무적·비재무적 손실이 발생하게 된다[9]. 이러한 기밀정보를 보호하기 위해서 기업들은 정보보안에 집중적으로 투자하고 있다. 정보보안은 기업의 정보를 안전하게 관리하는 장치이며, 기밀정보가 누설되지 않도록 보호·관리하는데 목적이 있다[10]. 정보보안 활동은 조직 내 개인과 관련되어 있으며, 기업의 정보보안 제도와 절차와도 관련되어 있다[8].

하지만 기업의 기밀 기술을 유출을 방지하기 위한 기술적 보안, 물리적 보안 등의 수많은 활동을 집중하고 있지만 기술 유출이 조직 내부의 개인으로 인해 발생하기도 한다[4]. 기업의 기밀정보 유출은 기업의 막대한 손실을 유발하기 때문에 국가 차원에서 피해를 효과적으로 대처하기 위해 법률도 제정하고 있으며, 안전한 산업 육성과 관리 차원에서 신경을 쓰고 있는 영역이다[11]. 산업기밀보호센터에 의하며 2022년에 첨단 자율주행 기술이 유출되는 사건이 있었으며, 2021년에는 2차전지 소재 분야 기술이 유출되는 사건이 있었다[12]. 이처럼 최신 기술에 대한 유출 사고가 발생하고 있다. 이에 정보보안 활동은 기업의 기밀정보 유출을 사전에 방지할 수 있는 경쟁력이라고 할 수 있다.

2.2 관리적 정보보안

정보보안은 <그림 1>처럼 세 가지 계층구조로 되

어 있으며, 관리적, 기술적, 물리적 보안으로 구분된다. 이중 관리적 보안은 최상단에 위치하여 물리적 보안과 기술적 보안의 행동 지침을 마련할 수 있는 구조로서 중요성을 가지고 있다[8]. 관리적 보안은 인적자원 관리, 정보자산 관리의 정책 및 제도를 중점으로 구성되어 있으며 무형적 가치의 요소를 내포하고 있다[13].



<그림 1> 정보보안의 계층적 구조

한편, Solms[14]는 정보보안을 기술적 보안만 강조할 것이 아니라 관리적 보안 활동에도 집중되어야 올바른 정보보호가 될 수 있다고 강조하였다. Hone과 Eloff[15] 또한 산업 정보보호 활동에서 기술적 보안과 함께 기업의 적절한 보안정책과 관리지침이 마련되어야 하고, 지속적인 지원을 통해 정보 취약점을 제거할 수 있어야 한다고 강조하였다. 이렇듯 관리적 보안은 기업의 기밀정보를 방지하기 위한 통제 활동으로 역할을 부여할 수 있다. 관리적 보안은 조직의 보안정책을 수립하고 권한·책임의 공식화, 보안사고 발생 시 대처 방법, 해킹 및 비인가 접근의 지속적 감시와 추적 마련, 물리적·기술적 보안 활동의 지원체계 마련을 제공하는 등 절차적이고 실체적인 보안 가이드라인을 정립하는 활동이라고 할 수 있다[16].

하지만 기업의 정보보안 운영이 체계적이고 실시간으로 구현되더라도 외부에 의한 재해 발생, 내부적인 과실과 고의성에 의해서 기밀정보는 언제든지 유출될 수 있다. 이에 성공적인 정보보안은 최고경영자부터 실무자까지 정보보안 인식이 높은 경우이며 특히 경영자는 정보보안에 관심을 가져야 한다[17].

2.3 정보보안의 준수 의도

조직 내 정보보안 준수 의도는 보호하고자 하는 자료와 정보를 위해서 사전에 발생 가능한 위협을 파악하고, 조직구성원이 자발적으로 해당 정보를 보호하고 관리하는 의지를 말한다[18]. 기업은 조직구성원들이 합리적으로 정보보안 정책을 준수시키려면 정보보안 사고를 방지할 수 있고 빠르게 해결할 수 있는 대책을 사전에 마련해야 한다. 여기서 보안대책은 두 가지 대책으로 구분된다. 첫 번째 절차적 대책은 보안정책 수립, 정보보안 인식 강화를 위한 교육프로그램 등이 있다. 두 번째 기술적 대책은 정보 접근 모니터링, 바이러스 및 해킹 방지 소프트웨어 등으로 구성되어 있다[19]. 이렇듯 보안대책은 정보보호를 위한 행동이 되겠다.

또한, 정보보안 준수 의도를 조직 내부와 외부에서 발생하는 보안 위협으로부터 기밀정보를 보호하려는 조직구성원의 의지라고도 한다[20]. 정보보안 준수 의도가 높을수록 조직은 정보 보안사고의 대응능력을 높일 수 있다. 조직 업무의 권한 분배와 위임, 비인가의 접근 등에 대해서 의사소통 체계를 구체화하고 업무 흐름 체계를 투명적으로 설계하면 조직 내부에서 발생하는 보안사고를 예방할 수 있다[6].

즉, 조직 내 구성원들의 조직문화, 고유업무 담당과 보안 교육프로그램 진행은 정보보안 준수 의도를 높일 수 있다[21]. 그리고 구성원들의 정보보안 준수 행동은 개인의 정보보안 인식을 자연스럽게 강화해 줄 것이다. 조직구성원들이 기밀정보를 공유하게 되는 비윤리적 행동에 노출되지 않도록 조직 내부에 감시 체계를 구축하면 윤리적 딜레마에 노출되지 않을 것이며 비자발적이라도 정보보안 준수 의도는 자연스럽게 높아질 수 있다[7].

Ⅲ. 연구방법론

3.1 연구 프로세스

본 연구는 기업 정보보안의 중요성을 강조하기 위하여 정보보안 투자에 영향을 미치는 중요요인이 무엇인지 분석할 것이다. 또한 산업별로 정보보안 투자 차이가 있는지도 살펴볼 것이다. 최근 첨단기술의 해킹 시도, 내부 직원의 기밀정보 유출 등이 지속해서 발생하고 있어서 본 연구를 통해 정보보안의 중요성을 다시금 강조하고자 한다.

본 연구는 총 4단계의 분석 프로세스를 진행하고자 한다. 연구 프로세스는 <그림 2>에 제시하였으며, 첫 번째 단계에서는 정보보안의 중요 투자요인을 분석하고, 나머지 세 단계는 산업별 정보보안 투자의 차이점을 확인할 것이다.

- 연구단계 1 : 정보보안을 강화하는데 중요한 변수는 무엇인가?

연구단계 1에서는 정보보안 규정을 준수하는데 중요한 핵심 변수가 무엇인지 분석할 것이다. 분석에서는 범주형 회귀분석을 활용하여 인과관계 분석으로 중요 독립변수를 분석할 것이다.

<표 1> 구성요인별 측정항목

변수명	아이템명		변수 구분	참고문헌
독립변수	정보보호 인식	귀사는 정보보호에 대하여 얼마나 중요하게 생각하십니까? ① 전혀 중요하지 않다 ~ ③ 보통이다 ~ ⑤ 매우 중요하다	5점 척도 구간변수	[5,6,7,8.14, 16, 22]
	개인정보보호 인식	귀사는 개인정보보호에 대하여 얼마나 중요하게 생각하십니까? ① 전혀 중요하지 않다 ~ ③ 보통이다 ~ ⑤ 매우 중요하다	5점척도 구간변수	
	정보보호 전담 조직 보유	정보보호 조직(전담 조직)이 있습니까? ① 예 ② 아니오	명목변수	
	개인정보보호 전담 조직 보유	개인정보 보 조직(전담 조직)이 있습니까? ① 예 ② 아니오	명목변수	
	정보보호 조직과 개인정보보호 조직 공동 운영	정보보호 조직과 개인정보보호 조직 공동 운영? ① 예 ② 아니오	명목변수	
	정보보호 인력투자	귀사의 IT 인력 중 정보보호(개인정보보호 포함) 담당 인력이 차지하는 비중은 어떻게 됩니까? ① 정보보호 담당 인력 없음 ② 1% 미만 ③ 1~3% 미만 ④ 3~5% 미만 ⑤ 5~7% 미만 ⑥ 7~10% 미만 ⑦ 10% 이상	순위변수	
	정보보호 예산투자	귀사의 2020년 1년간 IT 예산 총액 중 정보보호(개인정보보호 포함) 관련 예산 비중은 몇 퍼센트(%)였습니까? ① 정보보호 예산 없음 ② 1% 미만 ③ 1~3% 미만 ④ 3~5% 미만 ⑤ 5~7% 미만 ⑥ 7~10% 미만 ⑦ 10% 이상	순위변수	
	기업규모	① 49명 이하 ② 50~249명 ③ 250명 이상	명목변수	
	업종(산업)	① 농림수산업 ② 제조업 ③ 건설업 ④ 도매 및 소매업 ⑤ 운수 및 창고업 ⑥ 숙박 및 음식점업 ⑦ 정보통신업 ⑧ 금융 및 보험업 ⑨ 부동산업 ⑩ 전문, 과학 및 기술서비스업 ⑪ 사업시설관리업 ⑫ 협회, 단체 수리 및 기타 서비스업 ⑬ 기타	명목변수	
종속변수	보안규정 준수	보안규정이 변경되거나 정책이 강화되었을 때 귀사의 조직구성원은 변경된 사항을 지키기 위해 얼마나 노력하고 있습니까? ① 전혀 그렇지 않다 ~ ③ 보통이다 ~ ⑤ 매우 그렇다	5점 척도 구간변수	

• 연구단계 2~4 : 산업별로 정보보안 준수, 담당 인력, 예산 비중에 대한 차이가 있는가?

연구단계 2~4에서는 산업별로 정보보안 투자에 대한 차이가 있는지를 세부적으로 분석할 것이다. 2단계에서는 보안규정 준수에 대한 산업별 차이를 분석하고, 3단계에서는 보안 담당 인력 보유 수준에 대한 차이를 분석할 것이다. 마지막 단계에서는 보안 예산 비중에 대한 산업별 차이를 분석할 것이다. 이를 위해 2~4단계까지는 대응분석을 시행하고자 한다.

<그림 2> 연구 프로세스

이러한 분석을 위해서 과학기술정보통신부와 한국정보보호산업협회에서 공개한 '2021년 정보보호 실태조사(기업)'의 데이터를 기초로 하였다[22]. 이 조사는 기업을 대상으로 표본 조사되었으며, 설문조사 기간은 2020년 12월 31일 기준으로 2021년에 조사된 데이터이다. 총 수집된 표본 수는 7,500개이다.

3.2 측정항목

연구 프로세스를 분석하기 위해서 다음의 <표 1>에 변수들을 제시하였다. 연구에서 사용되는 핵심 변수로는 정보보호 인식, 개인정보보호 인식, 정보보호 전담 조직 보유, 개인정보보호 전담 조직 보유, 정보보호 조직과 개인정보보호 조직 공동 운영, 정보보호 인력투자, 정보보호 예산투자, 기업규모, 업종(산업), 보안규정 준수 등으로 구성하였다. 각 변수는 구간변수, 명목변수, 순위변수 등으로 구성되어 있다.

IV. 연구 결과

4.1 표본의 특성

본 연구의 표본의 특성을 살펴보기 위해서 빈도분석을 수행하였고, 이는 <표 2>에 제시하였다.

산업은 제조업이 942개(12.6%)로 가장 높게 나타났다. 기업규모는 49명 이하가 4,476개(59.7%)로 가장 높게 나타났다. 기업들의 정보보호 정책 여부는 보유하고 있다가 3,877개(51.7%)로 높게 나타났다. 개인정보보호 정책 여부의 보유는 보유하고 있다가 4,018개(53.6%)로 높게 나타났다.

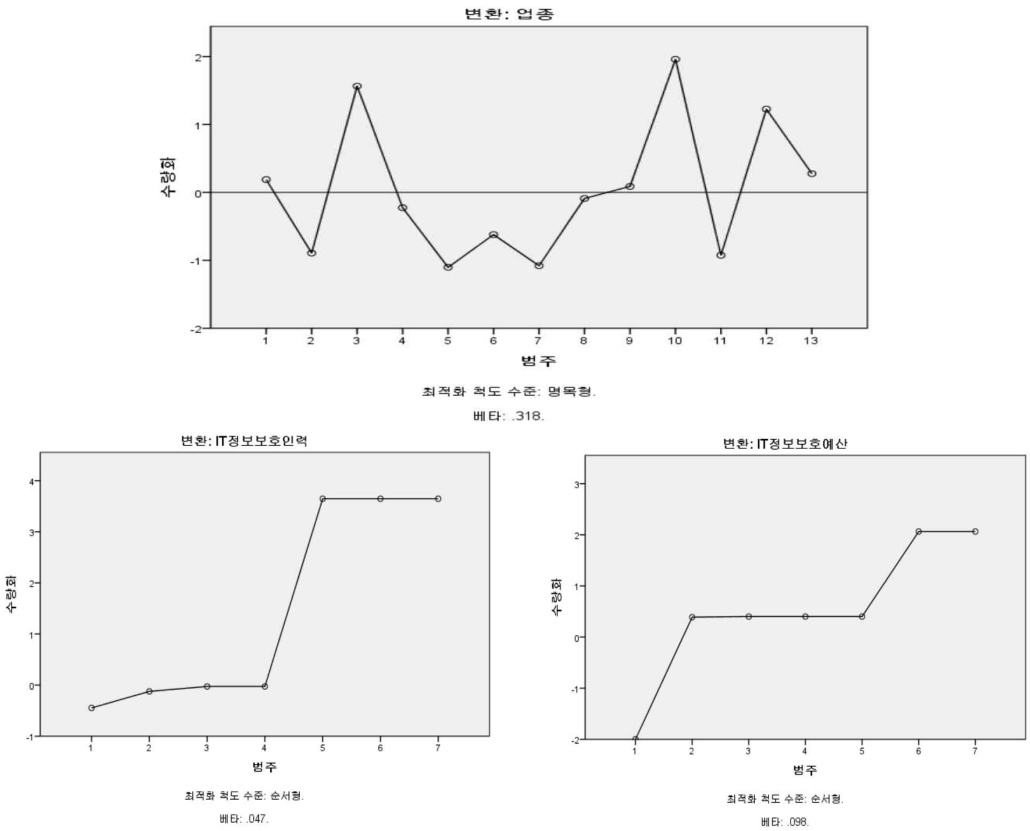
<표 2> 표본의 특성

구분		빈도	비율
업종 (산업)	농림수산업	242	3.2
	제조업	942	12.6
	건설업	684	9.1
	도매 및 소매업	799	10.7
	운수 및 창고업	504	6.7
	숙박 및 음식점업	484	6.5
	정보통신업	523	7.0
	금융 및 보험업	415	5.5
	부동산업	410	5.5
	전문, 과학 및 기술서비스업	619	8.3
	사업시설관리업	656	8.7
	협회, 단체 수리 및 기타 서비스업	404	5.4
	기타	818	10.9
기업 규모	49명 이하	4476	59.7
	50~249명	1748	23.3
	250명 이상	1276	17.0
정보보호 정책 여부	예	3877	51.7
	아니오	3623	48.3
개인정보보호 정책 여부	예	4018	53.6
	아니오	3482	46.4

<표 3> 정보보안 보안규정 준수 결과 – 범주형 회귀분석 결과

독립변수명	표준화 계수(베타)	F	유의확률	중요도
정보보호 인식	.130	44.186	.000	.164
개인정보보호 인식	.233	183.152	.000	.293
정보보호 전담 조직 보유	.014	1.845	.174	.005
개인정보보호 전담 조직 보유	.007	0.697	.404	.003
정보보호 조직과 개인정보보호 조직 공동 운영	.064	33.606	.000	.016
정보보호 인력투자	.047	15.250	.000	.028
정보보호 예산투자	.098	31.606	.000	.065
기업규모	.110	101.030	.000	.061
업종(산업)	.318	975.161	.000	.366

다중 R : 0.605, R 제곱 : 0.366, 수정된 R 제곱 : 0.364, F(p) : 172.446(0.000)



<그림 3> 정보보안 보안규정 준수 결과

4.2 연구 프로세스 분석 : 1 단계

본 분석을 위해서 범주형 회귀분석을 사용하였다. 범주형 회귀분석은 최소제곱법을 이용하여 명목형, 순서형, 수치형 등 혼합된 척도를 최적화를 수행하여 최적화된 선형 회귀식을 구할 수 있다[23]. 범주형 회귀분석을 통해서 창업에 필요한 중요요인이 무엇인지를 확인할 것이다.

이를 분석하고자 보안규정 준수를 종속변수를 설정하였다. 독립변수로는 정보보호 인식, 개인정보보호 인식, 정보보호 전담 조직 보유, 개인정보보호 전담 조직 보유, 정보보호 조직과 개인정보보호 조직 공동 운영, 정보보호 인력투자, 정보보호 예산투자, 기업규모, 산업을 선택하여 범주형 회귀분석을 실시하였다. 회귀 결과의 내용은 <표 3>에 제시하였다.

회귀분석의 설명력은 다중 R 값은 0.605이며, R 제곱은 0.366, 수정된 R 제곱은 0.364로 나타났다. F값은 172.446이며 p-value 값은 0.000으로 나타나 회귀모형은 적합하다고 나타났다.

분석 결과를 살펴보면 정보보호 인식의 베타 값은 0.130(p=0.000)으로 나타났고, 개인정보보호 인식의 베타 값은 0.233(p=0.000)으로 나타나 유의미한 인과관계 효과가 있다고 나타났다. 정보보호 전담 조직 보유와 개인정보보호 전담 조직 보유에 대한 베타 값은 1.845(p=0.174), 0.697(p=0.404)로 나타나 유의미한 인과관계가 없다고 나타났다. 정보보호 조직과 개인정보보호 조직 공동 운영의 베타 값은 0.064(p=0.000)로 나타나 유의미한 효과가 있다고 나타났다. 정보보호 인력투자와 정보보호 예산투자는 각각 베타 값이 0.047(p=0.000), 0.098(p=0.000)로 나타나 유의미한 인과관계가 있다고 나타났다. 기업규모와 산업(업종)의 각각 베타 값이 0.110(p=0.000), 0.318(p=0.000)로 나타나 유의미한 인과관계가 있다고 나타났다. 정보보호 보안규정 준수에 중요한 변수를 살펴보면 업종(산업), 개인정보보호 인식, 정보보호 인식 순으로 가장 높은 영향력을 가진다고 나타났다.

<그림 3>에서 업종(산업)을 세부적으로 살펴보면 10번 과학기술서비스업이 가장 큰 값을 보여주고 있으며, 다음으로 3번 건설업, 12번 협회단체업 순으로 보여주고 있다. 5번 운수 및 창고업, 7번 정보통신업의 경우에는 정보보안 준수 규정에서 과학기술서비스업보다는 낮은 값을 보여주고 있다. 특히 수량화 0을 기준으로 2번 제조업, 5번 운수 및 창고업, 7번 정보통신업, 11번 사업시설관리업, 6번 숙박 및 음식점업, 4번 도매 및 소매업, 8번 금융 및 보험업은 음의 수량에 위치해 있어서, 양의 수량에 위치한 과학기술서비스업과 건설업보다 정보보안 준수 규정에 낮은 산업군이라고 확인할 수 있다. 정보보호 인력투자를 세부적으로 살펴보면 5, 6, 7번의 차트 선이 수량화 4에 가까이 위치하고 있다. 이는 조직 내부에 5% 이상 담당 인력이 있는 경우 정보보안 규정 준수는 더욱더 효과적이라는 것을 설명하는 것이다. 정보보호 예산을 살펴보면 6번과 7번이 가장 높게 나타나 7% 이상 예산투자를 하는 기업이 보안규정 준수에 더욱더 적극적이라는 것을 설명할 수 있겠다.

4.3 대응분석 : 연구 프로세스 2~4 단계 분석

대응분석(Correspondence analysis)은 분할표 자료에 대하여 행과 열 범주 간 유사성, 연관관계, 상호관련성을 파악하기 위한 통계적 방법이다[24]. 즉, 범주형으로 관측된 두 변수 간의 관계를 다차원 공간상에서 도식적으로 파악하고자 할 때 유용하다[23, 24].

대응분석의 분할표의 행과 열, 행과 행, 열과 열의 관계를 분석하여 그 결과를 표와 차트로 제공한다[25]. 대응분석에서는 비슷한 열의 구성이 되는 행끼리는 가깝게 배치되고 비슷한 행의 구성이 되는 열끼리는 가깝게 배치되어 관계가 강한 행과 열은 가까이 배치되도록 좌표의 수치를 산출하고 있다[25].

4.3.1 연구 프로세스 2 단계 분석 : 산업별 보안규정 준수 차이 분석

전체 모형에 관한 데이터와 각 행 데이터에 관한 값들이다. <표 4>에 있는 값을 확인해보면 차원 1의 관성은 0.285로서 약 87.8%의 설명력을 가지고 있다. 두 번째 차원의 관성은 0.032로서 10% 정도의 설명력이 있다. 그러나 세 번째 차원의 관성은 그 값도 매우

작으며 설명력도 낮다. 따라서 인지도를 그리는 데 있어 2차원이면 충분하겠다. 또한 차원들의 카이제곱 값은 2434.504이며 p-value 값은 0.000으로 유의미한 차이가 있다고 나타났다.

<표 4> 산업별 보안규정 준수 - 대응분석

차원	비정칙값	요약 관성	설명 비율	누적 비율
1	.534	.285	.878	.878
2	.180	.032	.100	.978
3	.081	.007	.020	.998
4	.027	.001	.002	1.000
전체		.325	1.000	1.000

카이제곱=2434.504, 자유도=48, p=0.000

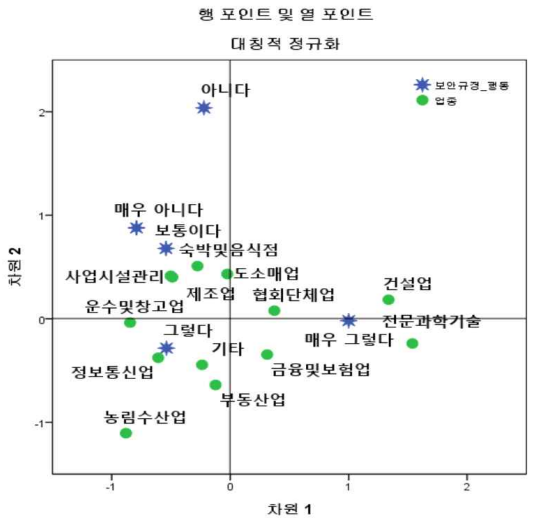
<표 5>의 행 포인트를 살펴보면 차원 1은 전문과학기술업, 건설업 순으로 중요하며, 차원 2는 부동산업, 제조업, 도소매업 순으로 기여도가 높은 것으로 나타났다. 열 포인트를 살펴보면 차원 1은 매우 그렇다, 그렇다가 기여도가 높게 나타났으며 차원 2에서는 보통이다, 아니다 순으로 높게 나타났다.

다음의 <그림 3>은 행과 열의 데이터를 토대로 인지로 표시한 결과이다. 인지도를 살펴보면 차원 2를 기준으로 하단에는 보안규정 준수에 그렇다와 매우 그렇다가 위치하고 있다. 상단에는 아니다, 매우 그렇다, 보통이 위치하고 있다. 차원 1의 우측에는 건설업, 과학기술, 금융 및 보험업, 협회단체업이 위치하고 있으며, 좌측에는 사업시설관리, 제조업, 운수 및 창고업 등이 위치하고 있다.

이중 건설업과 전문/과학기술서비스업은 정보 보안규정 준수에 대해서 매우 그렇다에 있으며, 정보통신업, 운수 및 창고업 등은 그렇다에 위치하고 있다. 숙박 및 음식업, 사업시설관리, 제조업 등은 보통이다에 위치하고 있다. 이러한 <그림 4>에 나타난 그룹군은 <그림 3>에 표현된 내용과 동일하게 나타났다.

<표 5> 산업별 보안규정 준수 - 행렬 분석

구분	업종(산업)	차원의 점수		기여도	
		1	2	1	2
행	농림수산업	-.880	-1.105	.047	.219
	제조업	-.488	.401	.056	.112
	건설업	1.336	.184	.305	.017
	도소매업	-.025	.432	.000	.111
	운수 및 창고업	-.845	-.037	.090	.001
	숙박 및 음식점업	-.276	.509	.009	.093
	정보통신업	-.608	-.376	.048	.055
	금융 및 보험업	.312	-.345	.010	.037
	부동산업	-.124	-.639	.002	.124
	전문/과학기술서비스업	1.538	-.238	.366	.026
	사업시설관리업	-.503	.415	.041	.084
	협회/단체업	.373	.078	.014	.002
	기타	-.237	-.445	.012	.120
열	매우 아니다	-.792	.878	.002	.007
	아니다	-.222	2.037	.001	.375
	보통이다	-.542	.680	.087	.404
	그렇다	-.539	-.283	.259	.213
	매우 그렇다	1.000	-.018	.651	.001



<그림 4> 산업별 보안규정 준수 인지도

4.3.2 연구 프로세스 3 단계 분석 : 산업별 정보보안 인력투자 차이 분석

다음으로 산업별 정보보안 인력투자에 대한 차이를 확인하고자 한다. <표 6>의 분석 결과를 살펴보면 차원 1의 관성은 0.235로서 약 56.2%의 설명력을 가지고 있다. 두 번째 차원의 관성은 0.098로서 23.4% 정도의 설명력이 있다. 그러나 세 번째 차원의 관성은 16% 미만으로 설명력도 낮다. 따라서 인지도를 표현하는 데 있어서 2차원이면 충분하겠다. 또한 차원들의 카이제곱값은 3139.600이며 p-value 값은 0.000으로 유의미한 차이가 있다고 나타났다.

<표 6> 산업별 정보보안 인력투자 - 대응분석

차원	비정칙값	요약 관성	설명 비율	누적 비율
1	.485	.235	.562	.562
2	.313	.098	.234	.796
3	.262	.069	.164	.960
4	.116	.013	.032	.992
5	.050	.003	.006	.998
6	.031	.001	.002	1.000
전체		.419	1.000	1.000

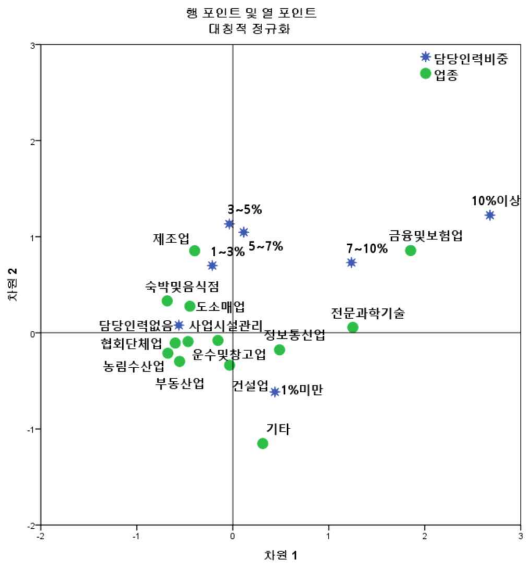
카이제곱=3139.600, 자유도=72, p=0.000

<표 7>의 행 포인트를 살펴보면 차원 1은 금융 및 보험업, 전문/과학기술서비스업 순으로 중요하며, 차원 2는 기타, 제조업 순으로 기여도가 높은 것으로 나타났다. 열 포인트를 살펴보면 차원 1은 10% 이상, 담당 인력이 없음의 순으로 나타났으며, 차원 2는 1% 미만, 3~5% 수준 순으로 나타났다.

이러한 결과를 토대로 두 가지 데이터를 하나의 인지도로 표시한 내용이 <그림 5>이다. 인지도를 살펴보면, 차원 2의 하단은 정보보안 인력이 없거나 낮은 비율의 인력을 보유한 산업을 보여주고 있으며, 상단은 정보보안 인력이 어느 정도 보유한 산업을 보인다. 차원 1을 기준으로 우측은 금융 및 보험업과

<표 7> 산업별 정보보안 인력투자 - 행렬 분석

구분	업종(산업)	차원의 점수		기여도	
		1	2	1	2
행	농림수산업	-.677	-.212	.030	.005
	제조업	-.397	.854	.041	.293
	건설업	-.033	-.336	.000	.033
	도소매업	-.447	.277	.044	.026
	운수 및 창고업	-.466	-.090	.030	.002
	숙박 및 음식점업	-.683	.333	.062	.023
	정보통신업	.487	-.177	.034	.007
	금융 및 보험업	1.853	.857	.392	.130
	부동산업	-.554	-.297	.035	.015
	전문/과학기술서비스업	1.251	.057	.266	.001
	사업시설관리업	-.155	-.079	.004	.002
	협회/단체업	-.599	-.106	.040	.002
	기타	.312	-1.152	.022	.462
열	담당 인력 없음	-.562	.079	.293	.009
	1% 미만	.439	-.615	.140	.427
	1~3% 미만	-.214	.700	.008	.131
	3~5% 미만	-.036	1.134	.000	.191
	5~7% 미만	.114	1.047	.000	.047
	7~10% 미만	1.236	.731	.067	.036
	10% 이상	2.679	1.224	.491	.159



<그림 5> 산업별 정보보안 인력투자 인지도

정보통신업 등이 있으며, 좌측에는 농림수산업과 부동산업, 협회/단체업 등이 위치하고 있다.

이 중 금융 및 보험업, 전문/과학기술서비스업은 7~10% 수준의 정보보안 인력을 유지하고 있다고 나타났다. 하지만 협회/단체업과 도소매업, 숙박 및 음식점업, 사업시설관리업은 정보보안을 담당하는 인력이 없다는 포인트 지점에 가까이 위치하고 있다. 즉, 산업별로 살펴보면, 정보보안이 상대적으로 중요한 금융 및 보험업과 전문/과학기술서비스업은 정보보안 인력투자를 강하게 하고 있다. 하지만 나머지 산업은 정보보안 인력투자에 인색한 형태를 보여주고 있다.

4.3.3 연구 프로세스 4 단계 분석 : 산업별 정보보안 예산투자 차이 분석

마지막으로 산업별 정보보안 예산투자에 대한 차이를 확인하고자 한다. <표 8>의 분석 결과를 살펴보면 차원 1의 관성은 0.186으로서 약 45.5%의 설명력을 가지고 있다. 두 번째 차원의 관성은 0.127로서 31.0% 정도의 설명력이 있다. 그러나 세 번째 차원의 관성은 6%로 설명력도 낮다. 따라서 인지도를 표현하는 데 있어서 2차원이면 충분하겠다. 또한 차원들의 카이제곱값은 3070.730이며 p-value 값은 0.000으로 유의미한 차이가 있다고 나타났다.

<표 8> 산업별 정보보안 예산투자 - 대응분석

차원	비정칙값	요약 관성	설명 비율	누적 비율
1	.432	.186	.455	.455
2	.356	.127	.310	.766
3	.246	.060	.148	.913
4	.138	.019	.047	.960
5	.101	.010	.025	.985
6	.079	.006	.015	1.000
전체		.409	1.000	1.000

카이제곱=3070.730, 자유도=72, p=0.000

<표 9>의 행 포인트를 살펴보면 차원 1은 금융 및 보험업이 가장 중요하며 다음으로 건설업 순으로 중요하다고 나타났다. 차원 2는 기타, 제조업, 도소매업 순으로 기여도가 높은 것으로 나타났다. 열 포인트를 살펴보면 차원 1은 10% 이상, 7~10% 미만 순으로 나타났으며, 차원 2는 1% 미만, 예산 없음, 3~5% 미만 순으로 나타났다.

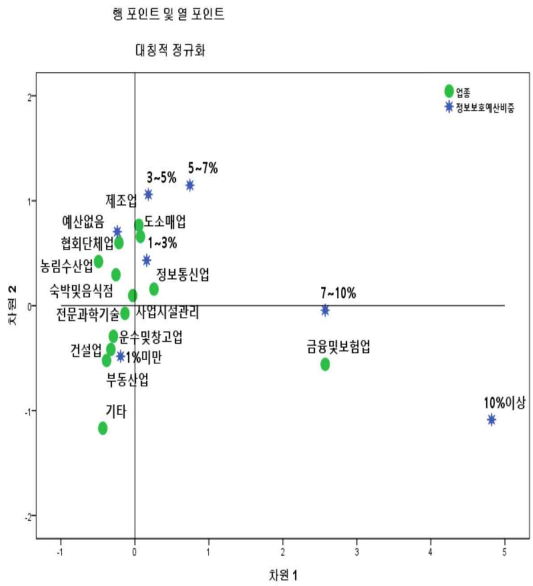
<표 9> 산업별 정보보안 예산투자 - 행열 분석

구분	업종(산업)	차원의 점수		기여도	
		1	2	1	2
행	농림수산업	-.492	.420	.018	.016
	제조업	.053	.766	.001	.207
	건설업	-.324	-.417	.022	.045
	도소매업	.075	.659	.001	.130
	운수 및 창고업	-.290	-.292	.013	.016
	숙박 및 음식점업	-.256	.295	.010	.016
	정보통신업	.258	.157	.011	.005
	금융 및 보험업	2.573	-.559	.848	.048
	부동산업	-.384	-.522	.019	.042
	전문/과학기술서비스업	-.134	-.074	.003	.001
	사업시설관리업	-.029	.096	.000	.002
	협회/단체업	-.216	.600	.006	.054
	기타	-.433	-1.169	.047	.418
열	예산 없음	-.238	.705	.025	.260
	1% 미만	-.194	-.482	.048	.364
	1~3% 미만	.159	.432	.008	.075
	3~5% 미만	.181	1.060	.005	.204
	5~7% 미만	.743	1.148	.022	.063
	7~10% 미만	2.572	-.043	.325	.000
	10% 이상	4.821	-1.087	.567	.035

이러한 결과를 토대로 나타낸 인지도의 그림은 <그림 6>에 표시하였다. 인지도의 내용을 살펴보면 차원 1을 기준으로 우측에는 금융 및 보험업이 위치하고 있으며, 좌측으로는 농림수산업, 숙박 및 음식점업, 건설업 등이 위치하고 있다. 차원 2를 기준으로 하단에는 건설업, 운수 및 창고업, 부동산업 등이 위

치하고 있으며, 상단에는 제조업, 도소매업, 협회단체업 등이 위치하고 있다.

이 중 금융 및 보험업은 7~10% 수준의 정보보안에 예산을 투자하고 있다고 나타났다. 정보통신업은 1~3%, 운수업, 건설업, 부동산업 등은 1% 미만의 예산을 투자하고 있다고 나타났다. 즉, 금융 및 보험업을 제외한 나머지 산업에서 정보보안 예산투자에 상당히 미흡한 수준이라는 것을 확인할 수 있다.



<그림 6> 산업별 정보보안 예산투자 인지도

V. 연구 결론

5.1 연구 결론과 이론적 함의

본 연구는 기밀정보 유출이 끊임없이 발생하고 있는 상황에서 산업별로 기업 정보보안 수준을 진단하는 연구였다. 기업들의 정보보안을 고민하지 않으면 내부정보의 관리가 소홀하게 되어 경쟁력을 상실하게 되거나 기업이 파산할 수 있는 경우도 발생하게 된다. 이러한 문제로 정보보안 투자의 중요성을 강조하고자 본 연구는 산업별로 정보보안 수준을 실증적으로 분석하였다. 분석에서는 범주형 회귀분석과 대응분석을 토대로 연구를 진행하였으며 결과를 요약하면 다음과 같다.

첫째, 정보보안 보안규정을 준수를 강화하는 데 도움이 되는 변수로 정보보호 인식, 개인정보보호 인식, 정보보호와 개인정보보호 공동 운영조직, 정보보호 인력투자, 정보보호 예산투자, 기업규모, 업종(산업) 등이 긍정적인 효과가 있다고 나타났다. 둘째, 보안규정 준수에 대한 산업별로 살펴보면 건설업과 전문과학기술업, 금융 및 보험업, 협회 단체업이 다른 산업에 비해 높은 보안규정 준수에 노력하고 있는 것으로 나타났다. 셋째, 정보보안 인력투자에 대한 산업별로 차이를 살펴보면 정보기술이 중요한 산업인 금융 및 보험업과 전문과학기술업에서 7~10% 수준의 정보보안 인력을 보유하고 투자하고 있다고 나타났다. 하지만 다른 산업은 1% 미만의 정보보안 인력을 유지하거나 담당 인력 자체가 없는 것으로 나타나 담당 인력의 편차가 높은 것으로 나타났다. 마지막, 정보보안 예산투자에 대한 산업별로 차이를 보면 금융 및 보험업의 경우 7~10% 수준의 정보보안 예산투자를 진행하고 있다고 나타났지만, 다른 업종(산업)의 경우 1~3% 미만 또는 1% 미만, 예산 자체가 없다고 나타나 대다수 업종(산업)이 정보보안 예산투자에 관심이 없다는 것으로 해석할 수 있겠다. 즉, 금융 및 보험산업은 전자금융감독규정에 따라 정보보호인력과 예산을 마련하고 있다고 볼 수 있다. 전자금융감독규정 제8조(인력, 조직 및 예산) 2항에서 정보기술 부문 인력은 총 임직원 수의 100분의 5 이상, 정보보호 인력은 정보기술 부문 인력의 100분의 5 이상이 되도록 할 것과 정보보호 예산을 정보기술 부문 예산의 100분의 7 이상이 되도록 권고하고 있다[26].

이러한 연구 결론을 토대로 이론적 함의는 다음과

같다. 첫째, 인공지능과 빅데이터가 중요한 정보자산으로 자리매김하고 있는 상황에서 정보보안 이론을 업데이트할 수 있는 기반을 마련하였다. 둘째, 정보보안의 중요성을 강조하면서 경영학 이론의 연구를 한 층 더 업데이트할 수 있었다. 마지막, 정보보안의 중요성을 강조하고자 범주형 회귀분석과 대응분석을 활용하면서 경영정보 연구의 통계적 방법론을 확대하는데 기여하였다.

5.2 실무적 함의

정보보안 투자를 진행하는 조직들의 실무적 함의는 다음과 같다. 첫째, 조직 내 강화된 정보보안 준수를 위해서 전담 조직 운영이 요구될 수 있다. 특히 대기업과 비교해 중소기업의 경우 인력 및 자본력의 부족으로 정보보안 관리가 더욱 취약하다. 중소기업은 핵심 인력의 이직 및 기밀정보의 복사와 이메일 전송이 대기업보다 높은 비율로 나타나[5] 이를 관리할 수 있는 전담 조직을 설치하거나 개인들의 정보보안 인식을 강조할 필요가 있겠다. 둘째, 산업별로 정보보안 인력투자와 예산투자의 편차를 줄이기 위해서 정부의 정보보안 투자 지원 및 정책적 마련이 요구될 수 있다. 특히, 정보보안 운영에 취한 중소기업과 벤처기업 등을 대상으로 정부 지원이 더욱 필요하겠다. 마지막, 기밀정보 유출 사고의 사례를 토대로 기업들은 수시로 교육훈련을 통해 정보보안 인식 강화를 높여야 할 필요가 있겠다.

5.3 향후 연구의 방향

본 연구는 2021년에 수집한 공공 빅데이터를 활용하여 산업별로 정보보안의 실태를 분석하고 차이점을 확인하였다. 하지만 2023년 시점에서 과거와 비교해 차이가 있는지 연구할 필요할 수 있겠으며, 추세 변화를 통해서도 새로운 시사점을 도출할 필요가 있겠다.

참고문헌

[1] 연합뉴스, 기술 경쟁 치열한데 또…삼성전자, '핵심자료 유출' 직원 해고, https://www.yna.co.kr/view/AKR20230516146700003?input=1195m, 2023-05-17

[2] 한국경제TV, 내부고발자 "테슬라, 개인정보 보호 안 해", https://www.wowtv.co.kr/NewsCenter/News/Read?articleId=A202305270046&t=NN, 2023-05-27

[3] 머니투데이, "삼성전자, 직원들 챗GPT 사용 금지"…회사정보 유출 차단, https://news.mt.co.kr/mtview.php?no=2023050210442436713, 2023-05-02

[4] 정병호, “비윤리적 정보공유 딜레마와 사회적 네트워킹 관계에서 정보접근 모니터링의 영향력,” 디지털산업정보학회 논문지, 제14호, 제2권, 2018, pp.91-105.

[5] 정병호, “기밀정보 유출 경험을 가진 기업들의 정보사고 대응역량 강화에 관한 연구,” 디지털정보산업학회지, 제12권, 제2호, 2016, pp.73-86.

[6] 이정환 · 정병호 · 김병초, “기업 보안 유형에 따른 보안사고 대응역량: 사회기술시스템 이론 관점에서,” 한국IT서비스학회지, 제12권, 제1호, 2013, pp.289-208.

[7] 정병호 · 김병초, “윤리 프로그램을 통한 비윤리적 정보공유 행동의 개선 : 사회적 자본과 잔물결 효과,” 디지털융복합연구, 제15권, 제8호, 2017, pp. 169-182.

[8] NIST, Information Security Handbook: A Guide for Managers, 2006.

[9] Merkow, Mark S., and Jim Breithaupt. Information security: Principles and practices. Pearson Education, 2014.

[10] Mattord, Herbert, and Michael Whitman.,

"Regulatory Compliance in Information Technology and Information Security," AMCIS 2007 Proceedings, 2007.

[11] 산업기술의 유출방지 및 보호에 관한 법률(약칭: 산업기술보호법), 시행 2023. 4. 4., https://www.law.go.kr/법령/산업기술의유출방지및보호에관한법률

[12] 산업기밀보호센터, https://www.nis.go.kr

[13] Baskerville, Richard, and Mikko Siponen., "An information security meta-policy for emergent organizations," Logistics Information Management, Vol.15, No.6, 2002, pp.337-346.

[14] Solms, B., "Information Security Management: The Second Generation.," Computer and Security. Vol.15, No.4, 1996, pp.281-288.

[15] Hone, K. & Eloff, J. H., "Information Security Policy: What do International Information Security Standards Say?.," Computers and Security, Vol.21, No.5, 2002, pp.402-409.

[16] Anderson, Evan E., and Joobin Choobineh., "Enterprise information security strategies," Computers & Security, Vol.27, No.1, 2008, pp. 22-29.

[17] Hu, Qing, et al., "Managing employee compliance with information security policies: the critical role of top management and organizational culture," Decision Sciences, Vol. 43, No.4, 2012, pp.615-660.

[18] Bulgurcu, B., Cavusoglu, H., & Benbasat, I., "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness," MIS quarterly, Vol.34, No.3, 2010,. pp.523-548.

[19] Hovav, A., & D'Arcy, J., "Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the US and South Korea," Information & Management, Vol.49, No.2, 2012, pp.99-110.

[20] Siponen, M., & Vance, A. "Neutralization: New insights into the problem of employee information systems security policy violations," MIS quarterly, Vol.34, No.3, 2010, pp.487-502.

[21] 황인호, "개인의 대처 유형과 조직문화가 조직원의 정보보안에 미치는 영향," 한국산업정보학회 논문지, 제26권, 제2호, 2021, pp.27-41.

[22] 과학기술정보통신부 · 한국정보보호산업협회, 2021년 정보보호 실태조사(기업), https://kisia.or.kr/

[23] 양경숙, SPSS를 이용한 최적 범주형 자료분석, 한나래아카데미, 2004.

[24] Hair, Joseph F., Multivariate data analysis, 2010.

[25] 노형진, SPSS에 의한 다변량 데이터의 통계분석, 효산출판사, 2007.

[26] 전자금융감독규정, 시행 2023.1.1. , https://www.law.go.kr/행정규칙/전자금융감독규정

■ 저자소개 ■

정 병 호
(Jung Byoungho)

2023년 현재 상지대학교 빅데이터사이언스학과 외래교수
2015년 8월 한국외국어대학교 경영학 박사
2011년 3월 한국외국어대학교 경영학 석사

관심분야 : IT투자, 정보윤리, 빅데이터, 신기술 혁신, 조직변화 관리
E-mail : jung.hmis@gmail.com

주 형 근
(Joo Hyungkun)

2023년 현재　한성대학교 교수
2021년 현재　기술표준원 평가위원. 상사중재인

관심분야 : e-비즈니스, 중소기업혁신
E-mail : hkjoo@hansung.ac.kr

논문접수일 : 2023년 6월 5일
수정접수일 : 2023년 6월 11일
게재확정일 : 2023년 6월 14일